What is claimed is:

1. A digital signing method, comprising:

applying a secret key to a message to generate a digital signature for the message;

distributing a digital-signature-attached message including the generated digital signature and the message;

registering the digital-signature-attached message as log data with a log list; and

providing said log list responsive to a request.

2. The digital signing method of claim 1, wherein said message is a hash value of another message.

3. The digital signing method of claim 1, wherein:

said applying a secret key to a message to generate a digital signature for the message further comprises:

applying said secret key to a message and data from a previously signed message retrieved from a recent log data registered in said log list to generate a digital signature for the message; and wherein:

said distributing a digital-signature-attached message including the generated digital signature and the message, further comprises:

distributing a digital-signature-attached message including the generated digital signature, the data from a previously signed message, and the message.

4. The digital signing method of claim 1, wherein said log data further comprises a distribution destination, and wherein:

said registering log data of the digital-signature-attached message with a log list further comprises:

registering log data of a digital-signature-attached message with a log list, said log data including a distribution destination attached thereto.

5. The digital signing method of claim 1, said method further comprising:

permitting registration of the log data with said log list only when the data from a previously signed message included in said digital-signature-attached message is included in the latest log data registered with said log list.

6. The digital signing method of claim 1, further comprising:

obtaining a timestamp from a trusted authority, said timestamp generated by applying a second secret key to the digital signature, and a time; and

said distributing a digital-signature-attached message including the generated digital signature and the message, further comprises:

distributing a digital-signature-attached message including the generated digital signature, the timestamp, and the message.

7. A digital signature verifying method, comprising:

accepting a digital-signature-attached message;

acquiring a log list of a digital signer, wherein said digital-signature-attached message may have been distributed by said digital signer is to be verified; and

checking whether log data of said digital-signature-attached message is registered in said log list, and

if the log data is registered in the log list, authenticating that the digital-signature-attached message was distributed by the digital signer.

8. The digital signature verifying method of claim 7, said method further comprising:

checking whether the digital signature included in the digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer.

9. The digital signature verifying method of claim 7, wherein said digital-signature-attached message further comprises data from a previously signed message, said method further comprising:

checking whether the digital signature included in the digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature, the data from a previously signed message,

and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer.

10. The digital signature verifying method of claim 9, said method further comprising:

checking whether data from a previously signed message included in said digital-signature-attached message is included in the log data registered immediately before log data of said digital-signature-attached message in said log list, and if the data from a previously signed message is included in the immediately previous registered log data, authenticating that said log list has not been altered.

11. The digital signature verifying method of claim 7, wherein said log data further comprises a distribution destination, said method further comprising:

acquiring a digital-signature-attached message from the distribution destination attached to the log data registered immediately before/after the log data of said digital-signature-attached message in said log list, and

checking whether the acquired message is included in said immediately previous/subsequent registered log data, and if the message is included, authenticating that said log list has not been altered.

12. The digital signature verifying method of claim 7, wherein said digital-signature-attached message further comprises a timestamp created using a second secret key, said method further comprising:

acquiring a digital signature and a time data by applying a public key paired with said second secret key to the timestamp included in said digital-signature-attached message; and

checking whether date and time indicated by the acquired time data exceeds a date and time of signing of said digital-signature-attached message, and if the date and time indicated by the time data does not exceed the date and time of signing of said digital-signature-attached message, authenticating the validity of the acquired digital signature.

13. A digital signing apparatus, comprising:

a processor; and

a storage medium; wherein said processor applies a secret key to a message to generate a digital signature for the message; and wherein

said processor prepares a digital-signature-attached message including the generated digital signature and the message; and wherein

said processor registers log data of said digital-signature-attached message with a log list in said storage medium.

14. The digital signing apparatus of claim 13, wherein, said message is a hash value of another message.

15. The digital signing apparatus of claim 13, wherein

said processor applies said secret key to a message and data from a previously signed message retrieved from a recent log data registered in said log list to generate a digital signature for the message; and wherein

said processor prepares a digital-signature-attached message that includes the generated digital signature, the message and the data from a previously signed message; and wherein

said processor registers log data of a digital-signature-attached message including the generated digital signature, the message, and the data from a previously signed message, with said log list.

16. The digital signing apparatus of claim 13, wherein said log data further comprises a distribution destination, and wherein:

said processor registers log data of a digital-signature-attached message with a log list, said log data including a distribution destination attached thereto.

17. The digital signing apparatus of claim 13, wherein:

registration of the log data with said log list is permitted only when the data from a previously signed message included in said digital-signature-attached message is included in the latest log data registered with said log list.

18. The digital signing apparatus of claim 13, wherein:

said processor obtains a timestamp from a trusted authority, said timestamp generated by applying a second secret key to the digital signature, and a time; and

said processor prepares said digital-signature-attached message including the generated digital signature, the timestamp, and the message.

19. The digital signing apparatus of claim 13, further comprising: an interface configured to be connectable to a computer.

20. The digital signing apparatus of claim 19, wherein:

if a number of the log data registered with the log list exceeds a particular value, said processor outputs at least one of a plurality of log data registered with the log list to said computer, whereupon said computer registers said at least one of a plurality of log data with a second log list prepared in said computer, and thereupon,

said processor deletes said at least one of a plurality of log data from said log list in said storage medium.

21. A digital signature verifying apparatus, comprising:

a processor interconnected with an input device, wherein:

said input device accepts a digital-signature-attached message to be verified and a log list of a digital signer; and wherein

said processor checks whether log data of said digital-signature-attached message is registered with said log list, and

if the log data is registered with the log list, authenticates that the digital-signature-attached message has been generated by said digital signer.

22. A digital signature verifying apparatus of claim 21, wherein:

said processor authenticates whether the digital signature included in said digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer.

23. A digital signature verifying apparatus of claim 21, wherein said digital-signature-attached message further comprises data from a previously signed message, and wherein

said processor authenticates whether the digital signature included in said digital-signature-attached message has been generated for the message included in the

digital-signature-attached message, using the digital signature, the data from a previously signed message, and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer.

24. A digital signature verifying apparatus of claim 23, wherein

said processor checks whether the data from a previously signed message included in said digital-signature-attached message is included in the log data registered immediately before the log data of said digital-signature-attached message in said log list, and if the data from a previously signed message is included in the immediately previous registered log data, said processor authenticates that said log list has not been altered.

25. The digital signature verifying apparatus of claim 21, wherein said log data further comprises a distribution destination, and wherein:

said processor acquires a digital-signature-attached message from the distribution destination attached to the log data registered immediately before/after the log data of said digital-signature-attached message in said log list, and wherein

said processor checks whether the acquired message is included in said immediately previous/subsequent registered log data, and if the message is included, said processor authenticates that said log list has not been altered.

26. The digital signature verifying apparatus of claim 21, wherein said digital-signature-attached message further comprises a timestamp created using a second secret key, and wherein:

said processor acquires a digital signature and a time data by applying a public key paired with said second secret key to the timestamp included in said digital-signature-attached message; and wherein

said processor checks whether date and time indicated by the acquired time data exceeds a date and time of signing of said digital-signature-attached message, and if the date and time indicated by the time data does not exceed the date and time of signing of said digital-signature-attached message, said processor authenticates the validity of the acquired digital signature.

27. A computer program product for creating a digital signature, said program product comprising:

code that applies a secret key to a message to generate a digital signature for the message;

code that prepares a digital-signature-attached message including the generated digital signature and the message;

code that registers log data of said digital-signature-attached message with a log list in said storage medium; and

a computer readable storage medium for embodying the codes.

28. A computer program product of claim 27, wherein the computer readable storage medium is a computer readable medium for storing the codes.

29. A computer program product of claim 27, wherein the computer readable storage medium is a computer readable medium for transmitting the codes.

30. A computer program product for verifying a digital signature, said computer program product comprising:

code that accepts a digital-signature-attached message and a log list from a digital signer; and

code that checks whether log data of said digital-signature-attached message is registered with said log list, and if the log data is registered with the log list, authenticates that the digital-signature-attached message has been generated by said digital signer; and

a computer readable storage medium for storing the codes.

31. A digital timestamp issuing apparatus, comprising:

a processor and an interface, wherein

said processor generates a timestamp by applying a secret key to data received by said interface, said data comprising a digital signature sent from a digital signer, and a reception time of the digital signature; and wherein

said processor transmits said timestamp to said digital signer using said interface.

32. A digital signing system, said system comprising:

a digital signing apparatus;

a timestamp issuing apparatus;

said digital signing apparatus comprising:

a processor and a communication interface, wherein said processor applies a first secret key to a message or its hash value to generate a digital signature; and

said processor transmits said digital signature to said timestamp issuing apparatus by said communication interface and acquires a timestamp in response; and wherein

said processor attaches the acquired timestamp to said message to create a digital-signature-attached message; and

said timestamp issuing apparatus comprising:

a processor and a communication interface, wherein

said processor generates a timestamp by applying a second secret key to data which includes the digital signature sent by said digital signing apparatus, and a reception time of the digital signature; and wherein said processor

transmits said timestamp to said digital signing apparatus.

33. The digital signing system of claim 32, said system further comprising:

a digital signature verifying apparatus comprising:

a processor interconnected with an input device, wherein

said input device accepts a digital-signature-attached message to be verified; and wherein

said processor acquires a digital signature and time data by applying a public key paired with the secret key of the timestamp apparatus to the timestamp included in said digital-signature-attached message; and thereupon,

said processor checks whether date and time indicated by the time data exceeds expiration date and time assigned at said digital signing apparatus, and when the date and time indicated by the time data does not exceed the expiration date and time, said processor authenticates the validity of the said digital signature; and thereupon,

said processor authenticates whether said digital signature included in said digital-signature-attached message has been generated for the message included in said digital-signature-attached message, using said digital signature, the message included in said digital-signature-attached message, and a public key paired with the secret key of the digital signing apparatus.